3Б

УДК 681.3

А.Я. Белецкий*, *А.А. Белецкий
Национальный авиационный университет, г. Киев, Украина
abelnau@ukr.net

RSB блочный криптографический алгоритм

Несмотря на многообразие существующих промышленных образцов блочных криптографических систем, все еще сохраняет актуальность разработка новых более гибких алгоритмов шифрования. Один из возможных вариантов построения таких алгоритмов рассматривается в данной статье [1], [2].

Общее описание *RSB* алгоритма

Аббревиатура ***RSB*** происходит от ключевых слов ***R**ound,* ***S**tep,* ***B**lok* – подчеркивая тем самым, что основными для криптоалгоритма являются раундовые преобразования, разбитые на определенное число шагов, а действие алгоритма осуществляется над блоками открытого или закрытого текстов. ***RSB*** – это итерационный блочный шифр, который доставляет уникальную возможность по изменению как размеров секретных ключей, так и числа шагов (раундов) шифрования. Отличительная особенность алгоритма состоит в том, что в нем используется функция шифрования типа *скользящего **RSB** кодирования*, которая обеспечивает не только глубокое перемешивание открытого текста, но и участвует в формировании *блочного раундового ключа* (определение дается ниже) для очередного шифруемого блока. Тем самым все преобразования, выполняемые криптоалгоритмом, становятся зависимыми не только от секретного ключа, но и от шифруемых данных, то есть относятся к классу «управляемых операций крипто-преобразования» или «управляемых криптопримитивов».

Алгоритм ***RSB*** предусматривает три варианта длины блока (для применения в различных классах безопасности) и переменную длину ключа шифрования для каждого варианта длины блока. Структура алгоритма ***RSB*** идентична для различных размеров блока, равных **128*n***, где ***n*** – коэффициент кратности длины блока, который может принимать значение **1,2** или **4**, то есть алгоритм поддерживает блоки, длиной 128, 256 и 512 бит. Описание ***RSB*** алгоритма приводится для длины блока 256 бит и отмечаются особенности реализации шифра для других размеров блока.

Основные параметры ***RSB*** алгоритма:

Размер блока – N = 128, 256 или 512 бит.

Длина раундового ключа – 32 бита.

Длина общего (шагового) ключа – $r*32$, $r=1, 2, ...$

Число шагов шифрования – $s=1, 2, ...$

Общее число раундов шифрования – $r*s$.

Размер элементов скользящего кодирования – 32 бита.

Размер элементов нелинейной замены – 8 бит.

Перед началом процедуры зашифрования входной открытый текст разбивается на блоки, размером в N бит. Если последний блок оказался меньше выбранного размера, то он дополняется (пробелами) до полного блока. Развернутая структурная схема ***RSB*** алгоритма в режиме зашифрования показана на рис. 1, где обозначено: RC (*Round Code*) – операции зашифрования текста раундовым ключом (подключом общего ключа); RK_{ij} – j-й базовый раундовый ключ на i-м шаге зашифрования.

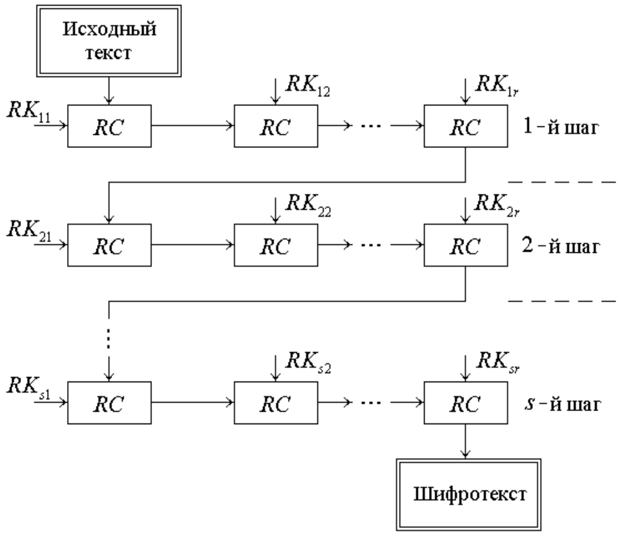


Рисунок 1 – Развернутая структурная схема ***RSB*** алгоритма в режиме зашифрования

Каждый раунд зашифрования ***RSB*** алгоритма включает следующую совокупность последовательно выполняемых криптографических примитивов:
– стохастическая круговая прокрутка шифруемого блока;
– скользящее кодирование 32-разрядных элементов блока;
– стохастическая нелинейная подстановка (замена) байтов блока;
– стохастическая перестановка элементов (слов) блока.

Перечисленные выше преобразования параметризуются с помощью блочного раундового ключа, структурная схема которого приведена на рис. 2.

31 C 24	23 S 16	15 β 8	7 P 0

Рисунок 2 – Структурная схема блочного раудового ключа

Блочные раундовые ключи меняются каждый раз при переходе к очередному преобразуемому блоку. Такая модификация ключей достигается за счет операции скользящего кодирования текста, содержащегося в предыдущих блоках. В силу отмеченной особенности 32-разрядные компоненты общего ключа шифрования выше названы *базовыми раундовыми ключами*, а результат их преобразования функцией скользящего кодирования будем называть *блочными раундовыми ключами.* Для первого блока шифруемого текста блочный раундовый ключ совпадает с базовым.

Далее приводится более подробное описание основных криптографических примитивов.

Стохастическая круговая прокрутка блока

Посредством данной операции осуществляется циклический сдвиг (круговая прокрутка) шифруемого блока на случайное нечетное число, которое задается восьмиразрядным двоичным байтом ***C*** (рис. 2). Семь старших разрядов этого байта считываются из сектора ***C*** блочного раундового ключа (разряды 31 – 25 на рис. 2), а в младший разряд формируемой кодовой комбинации принудительно записывается единица. Тем самым код, которым определяется порядок циклического сдвига блока, будет содержать нечетное число в интервале от 1 до 255.

Скользящее кодирование 32-разрядных элементов блока

Операция скользящего кодирования выполняет в ***RSB*** криптоалгоритме двойную роль. Во-первых, она обеспечивает достаточно глубокое *перемешивание* преобразуемого текста, цель которого состоит в том, чтобы сделать как можно более сложной зависимость между ключом и шифротекстом. И, во-вторых, с помощью такой операции осуществляется модификация блочных раундовых ключей, под управлением которых выполняются функциональные преобразования блоков текста, начиная со второго. В результате такой модификации блочный раундовый ключ i-го блока ($i > 1$) становится зависимым как от исходного базового раундового ключа RK_j, под управлением которого осуществляются преобразования первого блока текста, так и от шифруемых данных всех предыдущих $(i-1)$-х блоков.

В ***RSB*** шифре реализованы два типа скользящего кодирования: лево- и правостороннее, причем *левостороннее скользящее кодирование* применяется на нечетных раундах шифрования, а *правостороннее* – на четных раундах. Структурная схема алгоритма прямого левостороннего скользящего кодирования (процесс преобразования текста осуществляется по направлению слева направо) на этапе зашифрования первого блока приведена на рис. 3, где $\oplus$ есть оператор поразрядного сложения по mod 2; R' – 32-разрядный исходный (базовый) раундовый ключ, принимающий значение RK_j ($j = \overline{1, r}$) на j-м раунде зашифрования, а R'' – раундовый ключ для второго шифруемого блока.

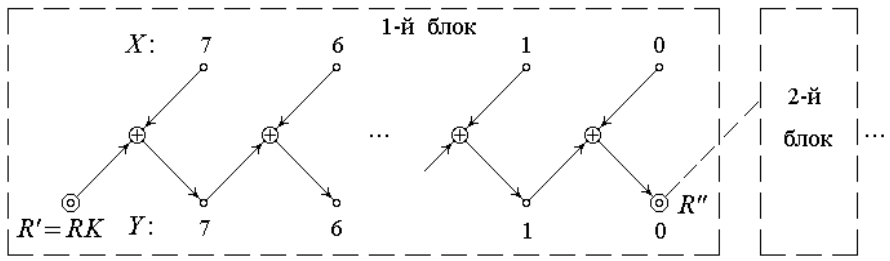


Рисунок 3 – Структурная схема алгоритма прямого левостороннего скользящего кодирования

Структурная схема алгоритма обратного левостороннего скользящего кодирования показана на рис. 4.

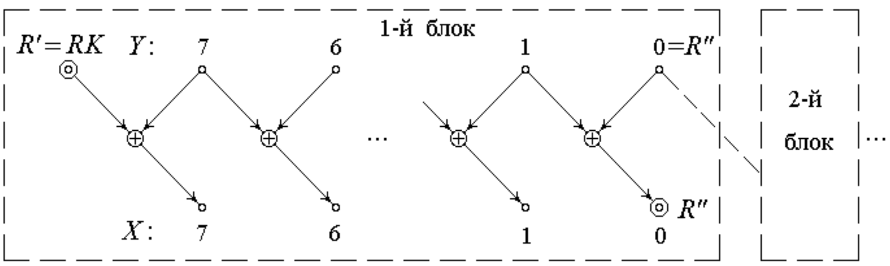


Рисунок 4 – Структурная схема алгоритма обратного левостороннего скользящего кодирования

Кроме левостороннего в ***RSB*** алгоритме применяется также правостороннее скользящее кодирование (для тех же целей, что и левостороннее); при этом процесс преобразования шифруемого текста осуществляется по направлению справа налево. Последняя отмеченная особенность ***RSB*** шифра является уникальной, не встречающейся ни в одном из известных блочных криптографических алгоритмов.

Нелинейная замена байтов

Схема построения S-боксов, посредством которых реализуются операции нелинейной замены байтов в ***RSB*** алгоритме, наследует основные черты S-боксов, принятых в ***AES*** шифре, и имеет вид:

$$y = (x \oplus S)^{-1} M \oplus \beta,$$

где S и β – байты блочного раундового ключа, показанного на рис. 2; M – инволютивная матрица преобразования; $\boldsymbol{x}^{-1}$ – восьмиразрядный элемент (байт), мультипликативно обратный байту $\boldsymbol{x}$ над выбранным неприводимым двоичным полиномом.

Стохастическая перестановка слов блока

С помощью этого криптографического примитива осуществляется стохастическая перестановка (перемешивание) двоичных слов в пределах шифруемого блока. В качестве слова в 128-разрядном блоке выступает байт, в 256-разрядном блоке словом является два, а в 512-разрядном – 4 байта, то есть каждый блок содержит 16 слов. Данная операция реализуется следующим образом. Например, в 128-разрядном блоке содержится 16 байтов, которым придадим десятичные номера от 0 до 15. Пусть $\boldsymbol{x}$ означает четырехразрядный двоичный номер байта шифруемого блока. Слово (байт), расположенный в ячейке блока, двоичный номер которой равен $\boldsymbol{x}$, перемещается в ячейку под номером $\boldsymbol{y}$, причем

$$y = (x \dot{\bullet} M_p)_2,$$

где $(a)_2$ означает приведение результатов поразрядного матричного произведения к остатку по mod 2, а M_p – матрица перестановки, в качестве которой выбирается одна из 16-ти инволютивных двоичных матриц четвертого порядка. Адрес A матрицы M_p содержится в секторе P блочного раундового ключа RK (рис. 2) и образуется по правилу:

$$P = p_1 \parallel p_2 \Rightarrow \boldsymbol{A} = \oplus \begin{matrix} p_1 \\ p_2 \end{matrix},$$

где p_1 и p_2 – полубайты сектора P.

Предлагаемый ***RSB*** алгоритм закладывает реальную основу для создания принципиально новой технологии симметричной блочной криптографической защиты информации в компьютерных сетях. Реализация данного проекта позволит существенно повысить криптостойкость систем шифрования по сравнению с уже существующими продуктами и в то же время сохранит высокую скорость криптопреобразования. Достижение первого отмеченного качества (криптостойкости) базируется на таких предпосылках. В сложившейся мировой практике построения симметричных блочных криптографических алгоритмов в пределах раунда все блоки шифруемого текста подвергаются одинаковым преобразованиям. С одной стороны, это обеспечивает возможность параллельной обработки информации, что повышает скорость шифрования. Вместе с тем если, например, в открытом тексте присутствуют одинаковые блоки, то одинаковыми будут также эти блоки после зашифрования, что облегчает работу криптоаналитиков. Отмеченный недостаток классических блочных шифраторов устраняется ***RSB*** технологией за счет применения двунаправленного скользящего кодирования, посредством которого каждый шифруемый блок текста становится управляемым своим индивидуальным блочным раундовым ключом, зависящим не только от базового раундового ключа, но и всего текста, предшествующего преобразуемому блоку. Высокую скорость шифрования в ***RSB*** технологии можно обеспечить за счет табличных и параллельных способов выполнения основных алгебраических преобразований, а также за счет аппаратной реализации на платформах с 32 или 64-разрядными шинами.

Выводы

1. ***RSB*** алгоритм допускает динамичное управление в широком диапозоне такими параметрами шифрования, как размер общего секретного ключа и число шагов (а, следовательно, и раундов) криптографических преобразований.

2. Криптографические преобразования в каждом блоке осуществляются под управлением индивидуальных локальных раундовых ключей, зависящих не только от значения секретного базового раундового ключа, но и всего текста, предшествующего преобразуемому блоку.

3. Основные выполняемые в ***RSB*** шифре криптографические преобразования (циклический сдвиг блока, скользящее кодирование 32-битных элементов, нелинейная подстановка байтов и перестановка слов в блоках) относятся к классу стохастических управляемых операций шифрования.

4. Стохастичность операций ***RSB*** шифрования обеспечивается не только выбором случайных базовых раундовых ключей, но и домешиванием в локальные раундовые ключи криптографически преобразуемых (в силу чего приобретающих стохастические свойства) 32-битных элементов шифруемого текста.

5. Табличный способ выполнения матричных преобразований обеспечивает ***RSB*** алгоритму достаточну высокую скорость шифрования.

6. ***RSB*** алгоритм допускает аппаратную реализацию на платформах с 32 или 64-разрядными шинами, причем возможно распараллеливание операций нелинейных подстановок байтов и перестановок слов в блоках шифрования.

7. Эффективность ***RSB*** алгоритма зашифрования, оцениваемая стандартным пакетом статистической оценки качества шифраторов ***NIST STS***, оказалось на уровне не ниже, а в отдельных случаях превышающем эффективность широко используемых стандартов криптографической защиты, таких, как ***DES***, ***ГОСТ***, ***AES*** и др.

Литература

1. Белецкий А.Я., Белецкий А.А. Симметричный блочный RSB-32 криптоалгоритм // Захист інформації. – 2006. – № 2 (29). – С. 42-51.
2. Белецкий А.Я., Белецкий А.А. Семейство симметричных блочных RSB криптографических алгоритмов с динамически управляемыми параметрами шифрования // Електроніка та системи управління. – 2007. – № 1 (11). – С. 5-16.
3. Молдавян А.А., Молдавян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры. – СПб.: БХВ – Петербург, 2002. – 496 с.

А.Я. Білецький, О.А. Білецький

RSB блочний криптографічний алгоритм

Недивлячись на багатоманітність існуючих промислових зразків блочних криптографічних систем, все ще зберігає актуальність розробки нових більш гнучких алгоритмів шифрування. Один з можливих варіантів побудови таких алгоритмів розглядається у даній статті [1], [2].

Статья поступила в редакцию 25.06.2008.